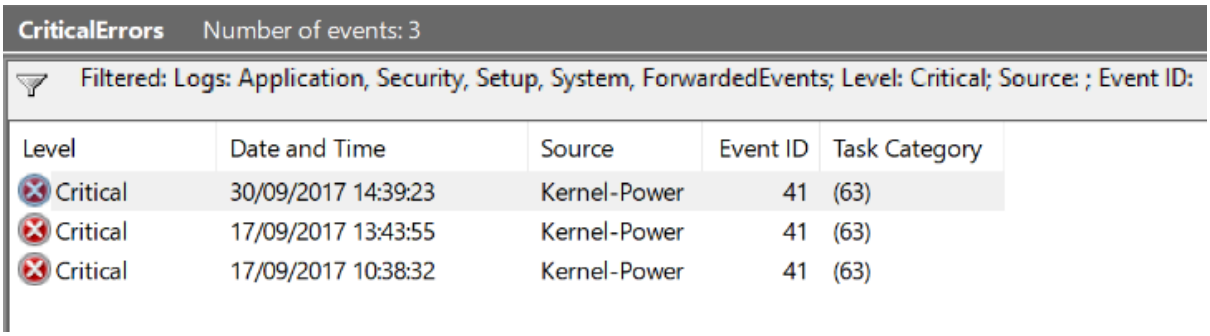
Forensic week 9

1. The Event Viewer is a part of the windows operating system. The event viewer allows users of the system to view the event logs on their local machine. This allows us to gather information on our system to see what hardware or software problems the user might be having. To start the event viewer, the quickest way is to press the windows key and r to bring up the run command we then type in “eventvwr”. When event viewer is, up and running we now want to see our critical errors on the system. To see our application critical errors, we click the windows logs drop down list and right click application. We then check the “Critical” box in the event level section and click ok. In the case of my system I have no application errors of a critical level. However, if we search all the windows logs, in the same way, we can see there is 3 critical errors in the system.



We can also filter by EventID but as there is only one error we wouldn’t get a different output. A critical error is error to say something has broken in the system and cause the system to crash at some point. As we can see from the source this is a kernel event / problem. The EventID 41 is given and when I investigated further if found out this means the system has rebooted without cleanly shutting down.

2. Two Companies that create hardware for mobile forensic data our Paraben and Cellebrite. The Paraben DS Tool box is a small kit that contains some cables and adapters for the phone. This kit also comes with a SIM card reader and micro media reader. This will allow the user to retrieve some sort of forensic information. However, this tool kit is very limited as there is more high end hardware available and the information that can be gathered is also limited as to what is actually on the phone as messages are not saved to the SIM anymore. The Cellebrite hardware used is the UFED Ultimate. This device allows us to unlock devices faster, decode data quickly and comprehensively, Access more data from a wider range of devices and Increase efficiencies to find evidence. This hardware does a lot of things however it does have limitations as it cannot export to a media friendly device. The price of this device would be astronomical and this device is also used by the military and law enforcement. It also requires specific training to use.

   As a device, just to use I would pick the Cellebrite UFED as it is more of a hacker's device and would give you most if not all the information available on the device. If the device has a pin/ pattern, password or anything of the nature this device can crack it. We can search a filter data to easily find the information we want. We can see the connections between the people, places and system. We can access live, hidden and deleted data from this device and keep it all intact. The UFED device can decode data faster and deeper into the phone and access the memory and take all the information the user needs. This device is a very powerful tool used by the military and law enforcement that can really make their lives easier and simpler.

Question 1:
https://www.isunshare.com/windows-10/6-ways-to-open-event-viewer-in-windows-10.html
https://support.microsoft.com/en-ie/help/2028504/windows-kernel-event-id-41-error-the-system-has-rebooted-without-clean
https://www.computerhope.com/jargon/e/evenview.htm
https://www.howtogeek.com/school/using-windows-admin-tools-like-a-pro/lesson3/

Question 2:
https://www.cellebrite.com/en/products/ufed-ultimate/
https://www.paraben.com/products/ds-toolbox